PAT-NO: JP02000182242A

DOCUMENT-IDENTIFIER: JP 2000182242 A

TITLE: METHOD AND DEVICE OPTICAL RECORDING, AND METHOD AND DEVICE FOR OPTICAL READING

PUBN-DATE: June 30, 2000

INVENTOR-INFORMATION:

NAME	COUNTRY
KONO, KATSUNORI	N/A
BABA, KAZUO	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
FUJI XEROX CO LTD	N/A

APPL-NO: JP10357635

APPL-DATE: December 16, 1998

INT-CL (IPC): G11B007/004 , B42D015/10

ABSTRACT:

PROBLEM TO BE SOLVED: To cipher and decipher data fast without spoiling the feature of high-speed transfer of a hologram memory.

SOLUTION: Ciphered object light is generated by exclusively ORing transmitted data to be ciphered and secret key data for ciphering and recorded as a hologram in an optical recording medium 10. For its read, the

optical recording medium 10 is irradiated with the same readout light 12 as the reference light for the recording and a reproduced image 11 is diffracted from the hologram to the optical path of the object light. At the same time, a secret key image 13 having a polarization direction orthogonal to the polarization direction of the reproduced image 11 is generated, transmitted through the optical recording medium 10, and imaged on the optical path of the reproduced image 11 to interfere with the reproduced image 11. A polarizer 42 is arranged on the common optical path of the reproduced image 11 and secret key image 13 and the direction of its transmission axis is made orthogonal to the direction of the composite vector of the polarized light of the reproduced image 11 and the polarized light of the secret key image 13. Consequently, a ciphered data image of exclusive OR between the reproduced image 11 and secret key image 13 is obtained as light having been transmitted through the polarizer 42.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the approach and equipment which read the approach of enciphering data and recording on an optical recording medium as a hologram, and the data which were equipment [data] and enciphered and were recorded on the optical recording medium as a hologram from an optical recording medium, and decrypt them.
[0002]
[Description of the Prior Art] The hologram memory which combines the large capacity nature originating in a three-dimension-record section and the rapidity originating in a two-dimensional package play back system as computer filing memory of the next generation in which mass record and fast transfer are possible attracts attention.
[0003] In a hologram memory, in the same volume, multiplex can be carried out, and two or more data pages can be recorded, and data can be collectively read for every page. Record playback of digital data also becomes possible by carrying out digital imaging of not an analog image but the binary digital data "0, 1" as "** and dark", and carrying out record playback as a hologram. Recently, the evaluation of an SN ratio or a bit error rate based on the concrete optical system of this digital hologram memory system and a volume multiplex recording method or the proposal about a two dimensional modulation is made, and the research from more nearly optical viewpoints, such as effect of the aberration of optical system, is also progressing.
[0004] The shift multiplex recording method which was shown in reference "D. Psaltis, M.Levene, A.Pu, G.Barbastathis and KCurtis;Opt.Lett.20 (1995) 782" at drawing 11 and which is an example of a volume multiplex recording method is shown.
[0005] By the shift multiplex recording method shown in this reference, the hologram record medium 91 is made into a disk configuration, the reference beam 96 of the spherical wave acquired through the objective lens 95 is irradiated at the hologram record medium 91, and overwrite of two or more holograms is carried out to the same field by rotation of the hologram record medium 91 at the same time it carries out the Fourier transform of the body light 93 obtained through the space optical modulator 92 with a lens 94 and irradiates the hologram record medium 91. For example, if a beam diameter is set to 1.5mmphi, another hologram to the almost same field can be recorded only by moving the dozens of micrometers hologram record medium 91, without producing a cross talk. Since a reference beam 96 is a spherical wave, this uses becoming that the include angle of a reference beam 96 changed with migration of the hologram record medium 91, and equivalence. According to this approach, the storage capacity of 100 times or more of CD is expectable.
[0006] By the way, since all the information by which disk package media, such as the present CD and DVD, are recorded on the disk is disclosed by the disk owner, when a disk owner receives a disk, it can use all the information currently recorded on the disk. Therefore, the unauthorized use and illegal copy (the so-called production of a pirate edition) by the disk owner with malice are possible.
[0007] A data encryption is effective as an approach of avoiding this problem and preventing an

unauthorized use and an illegal copy. For example, the cryptographic key generation method and the optical disk playback approach of preventing unauthorized uses and illegal copies of an optical disk, such as DVD, are shown in JP,10-149619,A. When the storage capacity of a disk increases and worth of the disk whose number is one will go up from now on, the unjust prevention by encryption is needed increasingly.
[0008]
[Problem(s) to be Solved by the Invention] Also when the hologram memory mentioned above spreads, naturally the problem of an unauthorized use or an illegal copy arises. Since the unit price of the disk of one sheet becomes high in proportion to the storage capacity, a pirate edition tends to overrun especially the hologram memory expected as a next-generation bulk memory, and protection of the data based on encryption becomes indispensable.
[0009] However, if the encryption approach proposed to current, DVD, etc. including the approach of above-mentioned JP,10-149619,A applies this to a hologram memory in order to perform electric serial processing, the fast transfer which is one of the features of a hologram memory will become impossible. Therefore, the approach of the high-speed encryption suitable for a hologram memory and a decryption is indispensable.
[0010] Moreover, only playback of the information as which the right private key was inputted can be permitted now by enciphering to a hologram memory, respectively and recording two or more information on it. Therefore, it becomes possible as an archive medium of a "superdistribution system" application which pays a countervalue to not "possession" but "use" of digital information to use a hologram memory. In this case, a user can obtain very cheaply the hologram memory on which immense information was recorded, can pay a countervalue and can reproduce only required information now.
[0011] Then, without spoiling the features of [when reading the data which this invention enciphers data and are recorded on an optical recording medium as a hologram and which were case / data / and enciphered and were recorded on the optical recording medium as a hologram from an optical recording medium and decrypting] the fast transfer of a hologram memory, data are enciphered at a high speed and it enables it to decrypt.
[0012]
[Means for Solving the Problem] By the optical recording approach of this invention, said body light is recorded as a hologram into that optical recording medium by generating the enciphered body light and irradiating that body light and reference beam at an optical recording medium at coincidence by the optical EXCLUSIVE OR operation of the transmission data to encipher and the private key data for encryption.
[0013] By the optical read approach of this invention, the enciphered body light reads to the optical recording medium currently recorded as a hologram, irradiates light, makes a playback image diffract from said hologram, and decrypts said body light by the optical EXCLUSIVE OR operation of that playback image and private key image.
[0014]
[Function] A cipher system is divided roughly into what uses a public key, and the thing using a private key (common key). Especially the latter private key also has a role like seal in a communication network, and will be used increasingly from now on. As technique using this private key, the exclusive OR of the data (plaintext) to encipher and a random key is calculated, and the approach of enciphering data is learned. However, in a hologram memory, if electric serial processing performs such EXCLUSIVE OR operation, the fast transfer which is one of the features of a hologram memory will become impossible.
[0015] On the other hand, by the optical recording approach of this invention by the above-mentioned approach, since this EXCLUSIVE OR operation is performed optically, generation and encryption of body light can be performed with the speed to which light progresses, and data can be enciphered to juxtaposition. Therefore, data can be enciphered and recorded on a high speed, without spoiling the features of the fast transfer of a hologram memory.
[0016] By the optical read approach of this invention by the above-mentioned approach, since

EXCLUSIVE OR operation for a decryption is performed optically similarly, data can be decrypted with the speed to which light progresses, and data can be decrypted to juxtaposition. Therefore, data can be decrypted and read at a high speed, without spoiling the features of the fast transfer of a hologram memory.
[0017]
[Embodiment of the Invention] [Operation gestalt of the optical recording approach] Drawing 1 is the case where an example of the optical recording approach of this invention is shown, perform optical EXCLUSIVE OR operation of the transmission data (plaintext) enciphered with the space optical modulators 21 and 22 and a polarizing plate (or 1/2 wavelength plate) 36, and the private key data for encryption, and the enciphered body light 1 is generated.
[0018] The space optical modulators 21 and 22 should form in two-dimensional many pixels in which polarization modulation is possible respectively. the space optical modulators 21 and 22 -- although the transmission data before encryption are inputted into the space optical modulator 21 and private key data are inputted into another side 22, for example, a space optical modulator, on the other hand, let the transmission data and private key data before the encryption be the two-dimensional binary digital data of an a large number bit, respectively. However, it is shown as 2x2 pixels thru/or 2x2 bits for convenience by a diagram.
[0019] As such space optical modulators 21 and 22, as shown in drawing 2 , the liquid crystal panel of the transparency mold in which electrodes 26 and 27 were formed to both sides of the electro-optics conversion members 25, such as liquid crystal, etc. is used. However, as space optical modulators 21 and 22, although a polarizing plate is arranged on the outside of electrodes 26 and 27, as shown in this drawing, that from which the polarizing plate was removed is used for the liquid crystal panel for projectors.
[0020] By this, the space optical modulators 21 and 22 can be operated as 1/2 wavelength plate which can make arbitration rotate polarization of incident light for every pixel, respectively.
[0021] And as shown in drawing 1 , first, a polarizing plate (or 1/2 wavelength plate) 33 is made to penetrate the coherent light 5, such as a laser beam made into parallel light, it is made into the linearly polarized light of the predetermined direction (below, the direction is made into 0 degree), and incidence of the linearly polarized light is carried out to the space optical modulator 21 inputted into the transmission data before encryption.
[0022] In this case, as the pixel as which the data "0" of the space optical modulator 21 were inputted is shown in drawing 3 (A), polarization of the light in which bearing of that 1/2 wavelength plate penetrates that pixel by becoming parallel to incidence polarization is not rotated. On the other hand, as the pixel as which the data "1" of the space optical modulator 21 were inputted is shown in drawing 3 (B), 45 degrees of bearings of the 1/2 wavelength plate incline to incidence polarization, and 90 degrees of polarization of the light which penetrates the pixel are rotated.
[0023] Therefore, as shown in drawing 1 , the body light 7 which has polarization distribution 7a according to the transmission data before encryption as a light which penetrated the space optical modulator 21 is obtained. Namely, the transmission data before encryption have a 0 degree (the direction of incidence polarization) polarization angle in the pixel of "0", and, as for the body light 7, the transmission data before encryption have a 90-degree polarization angle by the pixel of "1."
[0024] Next, incidence of the body light 7 before the encryption from this space optical modulator 21 is carried out to the space optical modulator 22 inputted into private key data.
[0025] Private key data are generated based on complicated code generation logic (algorithm), in order to raise security. The well-known encryption approaches, such as DES (Data Encryption Standard), FEAL (Fast Data Encipherment Algorithm), and RSA (Rivest-Shamir-Adleman), may be used for encryption, and it can use the encryption approach of arbitration.
[0026] As for the pixel as which the data "0" of the space optical modulator 22 were inputted, bearing of the 1/2 wavelength plate does not rotate polarization of parallel or the light which becomes perpendicular and penetrates the pixel to incidence polarization like the space optical modulator 21. On the other hand, 90 degrees of polarization of the light in which 45 degrees of bearings of the 1/2

wavelength plate incline to incidence polarization, and the pixel as which the data "1" of the space optical modulator 22 were inputted penetrates the pixel are rotated.
[0027] Therefore, the body light 8 to which polarization modulation of the body light 7 before the encryption from the space optical modulator 21 was carried out as a light which penetrated the space optical modulator 22 according to private key data, i.e., the body light which has polarization distribution 8a enciphered with private key data, is obtained.
[0028] Furthermore, a polarizing plate 36 is made to penetrate the body light 8 enciphered by the polarization distribution from this space optical modulator 22, and only the polarization component of a 90-degree polarization angle is taken out.
[0029] Therefore, the pixel as which data "0" were inputted into the space optical modulators 21 and 22 as a light which penetrated the polarizing plate 36, respectively, or in the pixel as which data "1" were inputted, respectively The pixel as which it became "dark" (optical reinforcement is zero), and data "1" were inputted into the space optical modulator 21, and data "0" were inputted into the space optical modulator 22, Or in the pixel as which data "0" were inputted into the space optical modulator 21, and data "1" were inputted into the space optical modulator 22, the enciphered body light 1 used as "**" (optical predetermined reinforcement) is obtained.
[0030] Namely, for every pixel, optical EXCLUSIVE OR operation of the transmission data before encryption and private key data is performed by juxtaposition, and the body light 1 enciphered according to intensity distribution is obtained.
[0031] And in parallel with it of the body light 1, in the above-mentioned example, the polarization direction irradiates the reference beam 2 of a 90-degree polarization angle to the field to which the body light 1 of an optical recording medium 10 is irradiated, and records the intensity distribution of the body light 1 as a hologram into an optical recording medium 10 at the same time it irradiates the body light 1 enciphered by these intensity distribution at an optical recording medium 10, as shown in drawing 4 .
[0032] Contrary to the example mentioned above, private key data may be inputted into the space optical modulator 21, and the transmission data before enciphering to the space optical modulator 22 may be inputted. Even in this case, the body light 8 which has the enciphered polarization distribution as a light which penetrated the space optical modulator 22 is obtained, and the body light 1 which has the enciphered intensity distribution as a light which penetrated the polarizing plate 36 is obtained.
[0033] As mentioned above, by the optical recording approach of this invention, generation and encryption of body light can be performed with the speed to which light progresses, and data can be enciphered to juxtaposition. Therefore, data can be enciphered and recorded on a high speed, without spoiling the features of the fast transfer of a hologram memory. For example, if the space optical modulators 21 and 22 shall be consisted of 1000x1000 pixels, respectively, generation and encryption of body light can be performed per 106-bit data at once.
[0034] [Operation gestalt of the optical read approach] At the time of read, as shown in drawing 5 , the body light 1 as which the optical recording medium 10 was enciphered reads to the field currently recorded as a hologram, and irradiates light 12. As a read-out light 12, the same light as the reference beam 2 at the time of record is used. The playback image 11 is diffracted on the optical path of the body light 1 from a hologram by this.
[0035] To coincidence, transmission data are decrypted this playback image 11 and by making it interfere in the private key image 13 of an opposite phase to this, and obtaining the image of the exclusive OR of the playback image 11 and the private key image 13. The private key image 13 is what considered the data "0" of the private key data used for the encryption at the time of record as optical OFF (dark), and considered data "1" as optical ON (**), for example, the space optical modulator and polarizing plate (or 1/2 wavelength plate) in which polarization modulation is possible can generate it.
[0036] Although there are an approach of adjusting the optical path difference between the playback image 11 and the private key image 13, an approach at least the optical-path top of the playback image 11 or the private key image 13 arranges a phase compensating plate, etc., as an approach of making an opposite phase the playback image 11 and the private key image 13 of each other, polarization is used in this example.

[0037] That is, as shown in drawing 5 , while carrying out image formation of the private key image 13 on the optical path of the playback image 11, the polarization direction of the playback image 11 and the polarization direction of the private key image 13 are made to cross at right angles. If the private key image 13 is generated using the space optical modulators 21 or 22 and polarizing plate 36 which were used at the time of record so that it may mention later, the private key image 13 will penetrate an optical recording medium 10 like drawing 5 , image formation will be automatically carried out on the optical path of the playback image 11, and it will interfere in it with the playback image 11.
[0038] And by arranging a polarizer 42 on the common optical path of this playback image 11 and the private key image 13, the image of the exclusive OR of the playback image 11 and the private key image 13 is obtained, and transmission data are decrypted.
[0039] That is, as shown in drawing 6 , the polarization direction of the playback image 11 and the polarization direction of the private key image 13 lie at right angles mutually. When the amplitude of the polarization of T1 and the private key image 13 by the amplitude of polarization of the playback image 11 was set to T2, the include angle theta to the polarization direction of the playback image 11 of the transparency shaft orientations of a polarizer 42 is made into 0 degree and the transparency shaft orientations of a polarizer 42 are made in agreement with the polarization direction of the playback image 11, the optical reinforcement which penetrates a polarizer 42 is proportional to |T1|2.
[0040] When an include angle theta is made into 90 degrees and the transparency shaft orientations of a polarizer 42 are made in agreement with the polarization direction of the private key image 13, the optical reinforcement which penetrates a polarizer 42 is proportional to |T2|2. Moreover, when the transparency shaft orientations of a polarizer 42 are made in agreement in the direction of the synthetic vector of polarization of the playback image 11, and polarization of the private key image 13, the optical reinforcement which penetrates a polarizer 42 is proportional to |T1+T2|2.
[0041] On the other hand, like drawing 6 , if the direction of the above-mentioned synthetic vector and the transparency shaft orientations of a polarizer 42 are made to cross at right angles, the optical reinforcement which penetrates a polarizer 42 will be proportional to |T1-T2|2, and as shown in drawing 7 , it will be obtained as a light which penetrated the polarizer 42, the image 14, i.e., the decrypted data image, of the exclusive OR of the playback image 11 and the private key image 13. When making equal the amplitude T1 and the amplitude T2, data can be decrypted by EXCLUSIVE OR operation optical in this way by making an include angle theta into 45 degrees.
[0042] A photodetector detects the decrypted data image 14 which penetrated this polarizer 42, and the transmission data before encryption are read. That is, the transmission data before encryption can be read by using the umbra of the decrypted data image 14 as data "0", and using a bright section as data "1."
[0043] When the private key data used for the encryption at the time of record and different data are inputted into the space optical modulator for private key image generation, the private key image 13 and the decrypted data image 14 as shown in drawing 7 are not obtained, and cannot read the transmission data before encryption. That is, only when the same data as the private key data used for the encryption at the time of record are inputted into the space optical modulator for private key image generation, the private key image 13 and the decrypted data image 14 as shown in drawing 7 are obtained, and the transmission data before encryption can be read.
[0044] As mentioned above, by the optical read approach of this invention, data can be decrypted with the speed to which light progresses, and data can be decrypted to juxtaposition. Therefore, data can be decrypted and read at a high speed, without spoiling the features of the fast transfer of a hologram memory.
[0045] [Operation gestalt of optical recording equipment] Drawing 8 shows an example of the optical recording equipment of this invention. Although what kind of thing may be used as an optical recording medium 10 as long as it can carry out hologram record, a photopolymer is used, for example. This example is the case where an optical recording medium 10 is made into a disk configuration.
[0046] The magnitude of 1 pixel uses the 640x480-pixel liquid crystal panel 1.3 mold for projectors for the space optical modulators 21 and 22 by 42micrometerx42micrometer. However, as mentioned above,

the thing except a polarizing plate is used.
[0047] Although what kind of thing may be used as long as it emits the coherent light which has sensibility in an optical recording medium 10 as the light source 30, 515nm of oscillation lines of an Ar ion laser is used, for example.
[0048] A beam splitter 31 divides the light from this light source 30 into the 2 flux of lights, it considers as polarization of the predetermined direction with a polarizing plate (or 1/2 wavelength plate) 33, and further, with lenses 34 and 35, light which penetrated the beam splitter 31 is made into the parallel light 6 with large aperture, and it carries out incidence to the space optical modulator 21.
[0049] The transmission data before encryption are inputted into the space optical modulator 21, and as shown and mentioned above to drawing 1 by this, to it, the body light 7 which has the polarization distribution according to the transmission data before encryption as a light which penetrated the space optical modulator 21 is obtained from a computer 51.
[0050] Incidence of the body light 7 before the encryption from this space optical modulator 21 is further carried out to the space optical modulator 22. In the space optical modulator 22, as the private key data for encryption are inputted and being shown and mentioned above from the computer 52 to drawing 1 by this, the body light 8 which has the polarization distribution enciphered with private key data as a light which penetrated the space optical modulator 22 is obtained.
[0051] Furthermore, as a polarizing plate (or 1/2 wavelength plate) 36 is made to penetrate the body light 8 enciphered by the polarization distribution from this space optical modulator 22 and it was shown and mentioned above to drawing 1, the body light 1 enciphered by intensity distribution is obtained as a light which penetrated the polarizing plate 36.
[0052] And the Fourier transform of the body light 1 enciphered by these intensity distribution is carried out with a lens 37, and an optical recording medium 10 is irradiated.
[0053] The light reflected in coincidence by the beam splitter 31 is reflected by mirrors 38 and 39, and the field to which the body light 1 of an optical recording medium 10 is irradiated is irradiated as a reference beam 2. However, the polarization direction of a reference beam 2 is made parallel with it of the body light 1. The intensity distribution of the body light 1 are recorded as a hologram into an optical recording medium 10 by this.
[0054] In this case, by rotating an optical recording medium 10 with the drive motor omitted by a diagram, a location can be changed into the hoop direction of an optical recording medium 10, and two or more holograms can be recorded on it. At this time, shift multiplex record can be performed by using a spherical wave as a reference beam 2. Furthermore, as the arrow head 71 of drawing 9 shows, as shown in this drawing, a hologram is recordable in forming a concentric circular recording track into an optical recording medium 10 by moving the optical recording head 70 in the direction of a path of an optical recording medium 10.
[0055] As mentioned above, with the optical recording equipment of this invention, generation and encryption of body light can be performed with the speed to which light progresses, and data can be enciphered to juxtaposition. Therefore, data can be enciphered and recorded on a high speed, without spoiling the features of the fast transfer of a hologram memory. Although it can encipher at once and 640x480-bit data can be recorded in the above-mentioned example, it is further accelerable by increasing further the number of pixels of the space optical modulators 21 and 22.
[0056] [Operation gestalt of an optical reader] Drawing 10 shows an example of the optical reader of this invention. The optical reader of this example adds the photodetector 43 for reading the polarizer 42 and the decrypted data image for the decryption by the lens 41 for an inverse Fourier transform, and EXCLUSIVE OR operation to the optical recording equipment of drawing 8 .
[0057] At the time of read, the same light as the reference beam at the time of record is irradiated as a read-out light 12 at an optical recording medium 10. As shown in drawing 5 , the playback image 11 is diffracted on the optical path of the body light 1 by this from the hologram currently recorded on the optical recording medium 10. With a lens 41, the inverse Fourier transform of the diffracted playback image 11 is carried out, and it is taken out.
[0058] Although a polarizing plate 33 is made to penetrate the light which penetrated the beam splitter

31, it is made into the parallel light 6 with large aperture with lenses 34 and 35 and the space optical modulator 21 is made it to carry out incidence to coincidence also at the time of read At the time of read, the data of all bits input the two-dimensional data of "0" (or "1") into the space optical modulator 21 from a computer 51. To the space optical modulator 22 From a computer 52, the private key data used for the encryption at the time of record are inputted, and the private key image 13 as shown in drawing 5 is generated as a light which penetrated the polarizing plate 36.
[0059] However, a polarizing plate 33, the data inputted into the space optical modulator 21, and a polarizing plate 36 are adjusted so that the polarization direction of the playback image 11 and the polarization direction of the private key image 13 may cross at right angles. The private key data used for the encryption at the time of record may be inputted into the space optical modulator 21, and the data of all bits may input the two-dimensional data of "0" (or "1") into the space optical modulator 22.
[0060] And carry out the Fourier transform of this private key image 13 with a lens 37, and an optical recording medium 10 is made to penetrate, and an inverse Fourier transform is carried out and it is made to interfere with the playback image 11 with a lens 41.
[0061] Therefore, as mentioned above in drawing 6 and drawing 7 , the data image 14 with which the exclusive OR of the playback image 11 and the private key image 13 was decrypted is obtained as a light which penetrated the polarizer 42 by making the direction of the synthetic vector of polarization of the playback image 11, and polarization of the private key image 13, and the transparency shaft orientations of a polarizer 42 cross at right angles. This decrypted data image 14 is detected by the photodetector 43, and the transmission data before encryption are read.
[0062] As mentioned above, in the optical reader of this invention, data can be decrypted with the speed to which light progresses, and data can be decrypted to juxtaposition. Therefore, data can be decrypted and read at a high speed, without spoiling the features of the fast transfer of a hologram memory. Although 640x480-bit data can be decrypted at once and can be read in the above-mentioned example, it is further accelerable by increasing further the number of pixels of the space optical modulators 21 and 22.
[0063]
[Effect of the Invention] As mentioned above, while being able to encipher and record data on a high speed according to this invention, without spoiling the features of the fast transfer of a hologram memory, the enciphered data can be decrypted and read at a high speed. And since data are enciphered and recorded, also when a hologram memory spreads through a world widely as memory in which mass record and fast transfer are possible, an unauthorized use and an illegal copy can be prevented. Moreover, it becomes possible as an archive medium of a "superdistribution system" application which pays a countervalue to not "possession" but "use" of digital information by encryption by restricting the data which can be read to use a hologram memory.

[Translation done.]